ELSEVIER

Theoretical Computer Science 235 (2000) 283–308

Theoretical Computer Science

www.elsevier.com/locate/tcs

extremal binary self-dual codes of length 40

Michio Ozeki

Department of Mathematics, Faculty of Science, Yamagata University, 1-4-12, Koshirakawa-chou, Yamagata, Japan

Abstract

In the present paper we develop a method to determine the coset weight distributions and covering radius of doubly even self-dual extremal binary codes of length 40. The method is algebraic in nature and largely eliminates necessary computations by electronic computers. The method easily applies to longer codes (e.g. self-dual [56, 28, 12] binary codes) or to non-extremal codes. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Code; Covering radius; Coset weight

1. Introduction

In [19] we introduced the notion of Jacobi polynomials for codes. After this paper, E. Bannai and the present author collaborated on the extension and the application of this notion. One main application of the notion is a construction of Jacobi forms via Jacobi's theta functions. (Announcements for this are stated in [3], and the full details will appear elsewhere.)

In the present paper we present another application of the notion of Jacobi polynomials for codes. Namely, we give a method for determining the covering radius of doubly even binary self-dual codes. The plan of the present paper goes in the following way. In Section 2 we collect some definitions and the notions necessary for later discussions. In Sections 3 and 4 we quote some well-known results and some not popular ones. In Section 5 we develop key propositions. In Section 6 we summarize some algebraic results. In Section 7 we describe explicit results.

Our present method gives first coset weight distribution of any coset with respect to a given code. As a consequence of it with a combination of some necessary computations we can determine the covering radius of binary self-dual codes. We remark that new ideas from polynomial approach of coding theory [3, 21, 4] enable us to predict some good information on codes. For instance, to determine the complete coset weight

E-mail address: ozeki@kszaoh3.kj.yamagata-u.ac.jp (M. Ozeki)

PII: S0304-3975(99)00200-5

distributions of an extremal binary self-dual code of length 40, it is enough to pursue some computations on the code words of weight 8 in the code. Although the results described in this paper are for extremal codes of length 40, our method also applies to the codes of other lengths, e.g. lengths 32, 56, 64 or to the non-extremal codes.

Finally, some words on other people's relevant works. Let $n=k+24r$ be the length of an extremal doubly even self-dual code $\mathscr{C}$. Delsarte's [10] work gives a method to determine coset weight distributions of coset weights up to i ($i=5$ if $k=0$, $i=3$ if $k=8$ and $i=1$ if $k=16$) by expanding certain polynomials $\beta(x)$ (in his notation) by means of Krawtchouk polynomials. Beyond that i one must appeal to computations to get the number of coset leaders in a given coset of weight i. Also to obtain the multiplicities of coset weight distributions one also has to compute with codewords. We remark that Delsarte [10] also gives sharp bounds for the covering radius of any linear codes.

Assmus and Pless [2] determined the covering radii of extremal doubly even binary self-dual codes of lengths 32 and 48. In case of length 48 the above-cited Delsarte's paper gives coset weight distributions of the extended quadratic code of length 48 and its covering radius. But there is an interesting open question whether there is an extremal doubly even binary self-dual code of length 48 other than quadratic residue type? (cf. [30, 14]) Assmus and Pless's result covers the general case of length 48. They also give an instance of complete coset weight distributions for doubly even binary self-dual code of length 32, namely extended quadratic residue code of length 32. Brualdi and Pless [6] initiated the case of length 40. Their result is rather indirect and shows the exitence of a doubly even binary self-dual code of length 40 having the covering radius 8.

2. Standard definitions from binary codes

Let $\mathbf{F}_2=GF(2)$ be the field of 2 elements. Let $V=\mathbf{F}_2^n$ be the vector space of dimension n over $\mathbf{F}_2$. A linear $[n,k]$ code $\mathbf{C}$ is a vector subspace of V of dimension k. In V, the inner product, which is denoted by $(\mathbf{x},\mathbf{y})$ for $\mathbf{x},\mathbf{y}$ in V, is defined as usual. Two codes $\mathbf{C}_1$ and $\mathbf{C}_2$ are said to be equivalent if and only if after a suitable change of coordinate positions of $\mathbf{C}_1$ all the codewords in both codes coincide. The dual code $\mathbf{C}^\perp$ of $\mathbf{C}$ is defined by

$$\mathbf{C}^\perp=\{\mathbf{u}\in V\mid(\mathbf{u},\mathbf{v})=\mathbf{0}\ \forall\mathbf{v}\in\mathbf{C}\}.$$

The code $\mathbf{C}$ is called self-orthogonal if it satisfies $\mathbf{C}\subseteq\mathbf{C}^\perp$, and the code $\mathbf{C}$ is called self-dual if it satisfies $\mathbf{C}=\mathbf{C}^\perp$.

Self-dual codes exist only if $n\equiv 0\,(\mathrm{mod})\,2$ and $k=n/2$.

An element $\mathbf{x}$ in $\mathbf{C}$ is called a codeword of $\mathbf{C}$. Let $\mathbf{x}$ be a codeword of a linear $[n,k]$ code $\mathbf{C}$ then the Hamming weight $wt(\mathbf{x})$ of the codeword

$$\mathbf{x}=(x_1,x_2,\ldots,x_n)$$

is defined to be the number of i's such that $x_i \neq 0$. The Hamming distance d on $\mathbf{C}$ is also defined by $d(\mathbf{x},\mathbf{y}) = wt(\mathbf{x}-\mathbf{y})$.

Let $\mathbf{C}$ be a self-dual binary $[n, n/2]$ code, then the weight $wt(\mathbf{x})$ of each codeword $\mathbf{x}$ in $\mathbf{C}$ is an even number. Further, if the weight of each codeword $\mathbf{x}$ in $\mathbf{C}$ is divisible by 4, then the code is called a doubly even binary code. It is known that doubly even self-dual binary codes $\mathbf{C}$ exist only when the length n of $\mathbf{C}$ is a multiple of 8.

The minimum distance $d(\mathbf{C})$ for a code $\mathbf{C}$ is defined by

$$d(\mathbf{C}) = \min_{\mathbf{u},\mathbf{v}\in\mathbf{C},\mathbf{u}\neq\mathbf{v}} d(\mathbf{u},\mathbf{v}) = \min_{\mathbf{u}\in\mathbf{C}-\{\mathbf{0}\}} wt(\mathbf{u}).$$

There is a well-known proposition:

Proposition 1. *Let* $\mathbf{C}$ *be a doubly even self-dual binary code of length* n; *then*

$$d(\mathbf{C}) \leqslant 4\left[\frac{n}{24}\right] + 4.$$

Definition. A doubly even self-dual binary code of length n satisfying

$$d(\mathbf{C}) = 4\left[\frac{n}{24}\right] + 4$$

is called an extremal code.

Let $\mathbf{C}$ be a self-dual doubly even code of length n, which is embedded in $\mathbf{F}_2^n$. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n), \mathbf{v} = (v_1, v_2, \ldots, v_n)$ be any pair of vectors in $\mathbf{F}_2^n$, then the number of common 1's of the corresponding coordinates for $\mathbf{u}$ and $\mathbf{v}$ is denoted by $\mathbf{u} * \mathbf{v}$. This is called the intersection number of $\mathbf{u}$ and $\mathbf{v}$, and $\mathbf{u} * \mathbf{u}$ is nothing else but $wt(\mathbf{u})$.

Let $\mathbf{C}$ be a doubly even self-dual binary $[n, n/2]$ code. The inhomogeneous weight enumerator $W_{\mathbf{C}}(X)$ of the code $\mathbf{C}$ is defined by

$$W_{\mathbf{C}}(X) = \sum_{\mathbf{v}\in\mathbf{C}} X^{wt(\mathbf{v})}.$$

If we denote by a_r the number of the codewords $\mathbf{v}$ of weight r in $\mathbf{C}$, then $W_{\mathbf{C}}(X)$ can be rewritten as

$$W_{\mathbf{C}}(X) = \sum_{r=0}^{n} a_r X^r.$$

For example, the Hamming code e_8 given in [20] has the weight enumerator

$$W_{e_8}(X) = 1 + 14X^4 + X^8.$$

We also give $W_{\mathscr{G}_{24}}(X)$ explicitly:

$$W_{\mathscr{G}_{24}}(X) = 1 + 759X^8 + 2576X^{12} + 759X^{16} + X^{24},$$

where $\mathscr{G}_{24}$ is the extended binary Golay code of length 24, and its generator matrix is given in [22].

Usually, the weight enumerator is expressed in the homogeneous form

$$W_{\mathbf{C}}(x, y) = \sum_{r=0}^{n} a_r x^{n-r} y^r.$$

Again, the homogeneous form of $W_{e_8}(X)$ is

$$W_{e_8}(x, y) = x^8 + 14x^4 y^4 + y^8.$$

But these two polynomials are mutually transformable into another forms by the rules

$$y^n W_{\mathbf{C}}\left(\frac{x}{y}\right) = W_{\mathbf{C}}(x, y)$$

and

$$y^{-n} W_{\mathbf{C}}(x, y) = W_{\mathbf{C}}(\xi) \quad \text{with } \xi = \frac{x}{y},$$

where n is the length of the code $\mathbf{C}$.

A basic result is the MacWilliams identity for binary self-dual code:

Theorem 1. *Let $W_{\mathbf{C}}(X)$ be the weight enumerator of a doubly even self-dual binary $[n, n/2]$ code; then the following identity holds*:

$$(1+X)^n W_{\mathbf{C}}\left(\frac{1-X}{1+X}\right) = |\mathbf{C}|\, W_{\mathbf{C}}(X).$$

We will use the subsets $\mathbf{C}_m$ of the code $\mathbf{C}$ defined by

$$\mathbf{C}_m = \{\mathbf{u} \mid wt(\mathbf{u}) = m\}.$$

A coset modulo a code $\mathbf{C}$ is an element of the vector space quotient $\mathbf{F}_2^n/\mathbf{C}$. Let $U = \mathbf{v}+\mathbf{C}$ be a coset modulo $\mathbf{C}$. A vector $\mathbf{v}$ in U is called a coset leader for U if the weight of $\mathbf{v}$ is minimal in the coset:

$$wt(\mathbf{v}) \leqslant wt(\mathbf{x}) \quad \forall \mathbf{x} \in U.$$

The weight of a coset is defined as the weight of the coset leader. Note that a coset may have more than one coset leaders.

We define the coset weight enumerator $W_U(X)$ for a coset U in $\mathbf{F}_2^n/\mathbf{C}$ by

$$W_U(X) = \sum_{\mathbf{x} \in U} X^{wt(\mathbf{x})}.$$

Let $\mathbf{C}$ be binary code of length n in $\mathbf{F}_2^n$. Let $S_r(\mathbf{x})$ be Hamming sphere of radius r with the center $\mathbf{x}$:

$$S_r(\mathbf{x}) = \{\mathbf{z} \in \mathbf{F}_2^n \mid d(\mathbf{z}, \mathbf{x}) \leqslant r\}.$$

An easy observation shows that the union of all $S_r(\mathbf{x})$, $\mathbf{x} \in \mathbf{C}$, covers the total space $\mathbf{F}_2^n$ when r is sufficiently large. The covering radius problem for the code $\mathbf{C}$ is to determine the least positive integer r so that the condition

$$\mathbf{F}_2^n = \bigcup_{\mathbf{x} \in \mathbf{C}} S_r(\mathbf{x})$$

holds. The solution for this problem is denoted by $t(\mathbf{C})$.

A reformulation of this problem is given by

Proposition 2. *It holds that*

$$t(\mathbf{C}) = \max_{\mathbf{u} \in \mathbf{F}_2^n} \left(\min_{\mathbf{z} \in \mathbf{u} + \mathbf{C}} wt(\mathbf{z}) \right).$$

A more precise problem is that for a given code $\mathbf{C}$ determine all the coset weight enumerators (or equally the coset weight distributions) $W_U(X)$.

We let $\mathbf{C}$ be a doubly even self-dual code of length n. Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbf{F}_2^n$; then $\mathbf{u} * \mathbf{v}$ is the intersection number of $\mathbf{u}$ and $\mathbf{v}$, as already explained directly after Proposition 1.

Definition of Jacobi polynomials for code. Jacobi polynomial $Jac(\mathbf{C}, \mathbf{v} \,|\, X, Z)$ for $\mathbf{C}$ with respect to $\mathbf{v} \in \mathbf{F}_2^n$ is defined by

$$Jac(\mathbf{C}, \mathbf{v} \,|\, X, Z) = \sum_{\mathbf{u} \in \mathbf{C}} X^{\mathbf{u} * \mathbf{u}} Z^{\mathbf{u} * \mathbf{v}}.$$

We will call the vector $\mathbf{v}$ the reference vector of the Jacobi polynomial in some occasions. The weight $wt(\mathbf{v})$ in the polynomial $Jac(\mathbf{C}, \mathbf{v} \,|\, X, Z)$ is called the index of the polynomial.

The polynomial $Jac(\mathbf{C}, \mathbf{v} \,|\, X, Z)$ may be expanded as

$$Jac(\mathbf{C}, \mathbf{v} \,|\, X, Z) = \sum_{m,r} b(m, r) X^m Z^r,$$

where $b(m, r)$ is given by

$$b(m, r) = |\{\mathbf{u} \in \mathbf{C} \,|\, \mathbf{u} * \mathbf{u} = m,\ \mathbf{u} * \mathbf{v} = r\}|,$$

where $|S|$ is the cardinality of a set S.

3. Quotation of some basic results

3.1. One known basic result

Let $\mathbb{C}[X]$ be the ring of all polynomials in one determinate X with coefficients in $\mathbb{C}$, the field of complex numbers. We denote by $\mathscr{W}[X]$ the subring of $\mathbb{C}[X]$ generated by the inhomogeneous weight enumerators attached to doubly even self-dual binary codes.

Theorem 2 (Gleason [12]). *$\mathscr{W}[X]$ has two polynomial generators $W_{e_8}(X)$ and $W_{\mathscr{G}_{24}}(X)$.*

3.2. Properties of Jacobi polynomials

Let $\mathbb{C}[X,Z]$ be the ring of all polynomials in two determinates X and Z, with coefficients in $\mathbb{C}$. Let $\mathbb{J}[X,Z]$ be the subring of $\mathbb{C}[X,Z]$ generated by Jacobi polynomials attached to doubly even self-dual binary codes.

As pointed in [21] we can regard

$$\mathbb{J}[X,Z] \supseteq \mathscr{W}[X].$$

First we give some elementary features of Jacobi polynomials for codes. All of them are quoted from [21].

Proposition 3. *Let* $Jac(\mathbf{C}_1, \mathbf{v}_1 \,|\, X,Z)$ *and* $Jac(\mathbf{C}_2, \mathbf{v}_2 \,|\, X,Z)$ *be two Jacobi polynomials; then we have*

$$Jac(\mathbf{C}_1, \mathbf{v}_1 \,|\, X,Z)Jac(\mathbf{C}_2, \mathbf{v}_2 \,|\, X,Z) = Jac(\mathbf{C}_1 \oplus \mathbf{C}_2, \mathbf{v}_1 \oplus \mathbf{v}_2 \,|\, X,Z).$$

Corollary 1 (to Proposition 3). *Let* $W_{\mathbf{C}_1}(X)$ *be the weight enumerator for a code* $\mathbf{C}_1$ *and* $Jac(\mathbf{C}_2, \mathbf{v} \,|\, X,Z)$ *be the Jacobi polynomial for another code* $\mathbf{C}_2$*; then the product* $W_{\mathbf{C}_1}(X)Jac(\mathbf{C}_2, \mathbf{v} \,|\, X,Z)$ *can be regarded as a Jacobi polynomial for the code* $\mathbf{C}_1 \oplus \mathbf{C}_2$ *with suitable vector* $\hat{\mathbf{v}}$:

$$W_{\mathbf{C}_1}(X)Jac(\mathbf{C}_2, \mathbf{v} \,|\, X,Z) = Jac(\mathbf{C}_1 \oplus \mathbf{C}_2, \hat{\mathbf{v}} \,|\, X,Z).$$

Thus $\mathbb{J}[X,Z]$ *is a* $\mathscr{W}[X]$*-module.*

Proposition 4. *Let the notations be as above. If*

$$Jac(\mathbf{C}, \mathbf{v} \,|\, X,Z) = \sum_{m=0}^{n} \sum_{r=0}^{k} b(m,r) X^m Z^r$$

is a Jacobi polynomial for a code $\mathbf{C}$ *with the reference vector* $\mathbf{v}$ *of weight* k*, then the coefficients* $b(m,r)$ *satisfy*

$$b(m,r) = b(n-m, k-r) \quad \text{for } 0 \leqslant m \leqslant n \text{ and } 0 \leqslant r \leqslant k.$$

Let $\mathbf{C}$ be a doubly even self-dual $[n, n/2]$ code. Let $\mathbf{v}$ be any vector in $\mathbf{F}^n$. We put $\hat{\mathbf{v}} = \mathbf{1} - \mathbf{v}$ and call it the complementary vector of $\mathbf{v}$. We have

Proposition 5. *Let the notations be as above. If*

$$Jac(\mathbf{C}, \mathbf{v} \,|\, X,Z) = \sum_{\mathbf{u} \in \mathbf{C}} X^{\mathbf{u}*\mathbf{u}} Z^{\mathbf{u}*\mathbf{v}} = \sum_{m,r} b(m,r) X^m Z^r$$

is a Jacobi polynomial for a code $\mathbf{C}$*, then*

$$Jac(\mathbf{C}, \hat{\mathbf{v}} \,|\, X,Z) = \sum_{m,r} b(m,r) X^m Z^{\mathbf{v}*\mathbf{v}-r}.$$

We quote a result in [21]:

Theorem 3. *Let* $\mathbf{C}$ *be an even self-dual binary code of length* n *and* $Jac(\mathbf{C},\mathbf{v}\,|\,X,Z)$ *a Jacobi polynomial for the code* $\mathbf{C}$ *with any binary vector* $\mathbf{v}\in\mathbf{F}_2^n$; *then it holds that*

$$Jac(\mathbf{C},\mathbf{v}\,|\,X,Z) = \frac{1}{|\mathbf{C}|}(1+X)^n\left(\frac{1+XZ}{1+X}\right)^{wt(\mathbf{v})} Jac\left(\mathbf{C},\mathbf{v}\,\middle|\,\frac{1-X}{1+X},\frac{(1-XZ)(1+X)}{(1+XZ)(1-X)}\right).$$

The inhomogeneous Jacobi polynomials are very convenient in using computer algebra, but the homogeneous Jacobi polynomials behave far more clearly than inhomogeneous ones when we investigate mathematical properties of them. We use the inhomogeneous and homogeneous Jacobi polynomials alternatively according to the circumstances.

The homogenization process is described by

$$\text{inhomogeneous polynomial} \to \text{homogeneous polynomial}$$
$$F(X,Z)\mapsto f(x,y,u,v)=\left(\frac{u}{x}\right)^k x^n F\left(\frac{y}{x},\frac{xv}{yu}\right).$$

Here k is the index of the polynomial.

We denote this correspondence by

$$hom(F(X,Z)) = f(x,y,u,v). \tag{1}$$

Example. From an inhomogeneous polynomial

$$F_1(X,Z) = 1 + X^4(7Z+7) + X^8 Z$$

we obtain a homogeneous one

$$hom(F_1(X,Z)) = f_1(x,y,u,v) = x^7u + 7x^3y^4u + 7x^4y^3v + y^7v.$$

In general, we know a relation [21]

$$Jac(\mathbf{C},\mathbf{v};x,y,u,v) = x^n\left(\frac{u}{x}\right)^{wt(\mathbf{v})} Jac\left(\mathbf{C},\mathbf{v}\,\middle|\,\left(\frac{y}{x}\right),\left(\frac{xv}{yu}\right)\right)$$
$$= \sum_{\mathbf{u}\in\mathbf{C}} x^{n-wt(\mathbf{v})-wt(\mathbf{u})+\mathbf{u}*\mathbf{v}} y^{wt(\mathbf{u})-\mathbf{u}*\mathbf{v}} u^{wt(\mathbf{v})-\mathbf{u}*\mathbf{v}} v^{\mathbf{u}*\mathbf{v}}.$$

The polynomial $Jac(\mathbf{C},\mathbf{v};x,y,u,v)$ is a homogeneous polynomial in four new variables x,y,u and v, and even partially homogeneous in u and v. For this polynomial $Jac(\mathbf{C},\mathbf{v};x,y,u,v)$, we have [21].

Theorem 4. *Let* $\mathbf{C}$ *be a self-dual binary code of length* n. *Under the above notations*

$$Jac(\mathbf{C},\mathbf{v};x,y,u,v) = \frac{1}{|\mathbf{C}|}Jac(\mathbf{C},\mathbf{v};x+y,x-y,u+v,u-v) \tag{2}$$

holds.

This theorem is a reformation of Theorem 3 above.

The converse process of the homogenization process is described as the dehomogenization process

$$\text{homogeneous polynomial} \to \text{inhomogeneous polynomial}$$
$$f(x,y,u,v) \mapsto f(1,X,1,ZX) = F(X,Z).$$

We denote this correspondence by

$$deh(f(x,y,u,v)) = F(X,Z). \tag{3}$$

Example. From a homogeneous polynomial

$$f_2(x,y,u,v) = (xv - yu)^4,$$

we get an inhomogeneous one

$$deh(f_2(x,y,u,v)) = F_2(X,Z) = (ZX - X)^4.$$

Remark 1. We should regard the degree with respect to X of the polynomial $(ZX - X)^4$ to be 8, since it relates to the homogeneous polynomial of degree 8. In general, we view an inhomogeneous polynomial in $\mathbb{J}[X,Z]$ of the form $a_pX^p f_p(Z) + \cdots + a_qX^q f_q(Z)$ $(0 \leqslant p \leqslant q)$ to be of degree $p+q$ with respect to the variable X. By this setting we see that the mappings *hom* and *deh* can be proved to be mutually inverse mappings.

We consider the transformation laws of the polynomial $Jac(\mathbf{C}, \mathbf{v}; x, y, u, v)$ more precisely when $\mathbf{C}$ is a doubly even self-dual binary code. Before doing this, we recall some facts about the homogeneous weight enumerators of self-dual codes $\mathbf{C}$ over the binary field. When $\mathbf{C}$ is a doubly even self-dual code, the homogeneous version of Theorem 1 reads as

$$\begin{aligned} W_{\mathbf{C}}(x,y) &= \frac{1}{2^{n/2}} W_{\mathbf{C}}(x+y, x-y) \\ &= W_{\mathbf{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right), \end{aligned} \tag{4}$$

where n is the length of the code $\mathbf{C}$. Since $\mathbf{C}$ is doubly even, each codeword $\mathbf{u}$ of $\mathbf{C}$ has weight divisible by 4, and we know that

$$W_{\mathbf{C}}(x, \mathrm{i}y) = W_{\mathbf{C}}(x,y). \tag{5}$$

Let G_1 be the group generated by

$$\sigma_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

This group is of order 192 and is known as No. 9 in Shephard–Todd's list in [26]. Eqs. (4) and (5) show that the homogeneous weight enumerator $W_{\mathbf{C}}(x,y)$ for a doubly

even self-dual binary code belongs to the ring of invariant polynomials $\mathbb{C}[x,y]^{G_1}$ for the finite group of linear transformations G_1. Let $\mathscr{W}[x,y]$ be the subring of $\mathbb{C}[x,y]$ generated by the homogeneous weight enumerators of doubly even self-dual binary codes. Then Gleason's theorem (Theorem 2) can be regarded as: the ring $\mathscr{W}[x,y]$ is a subring of the ring $\mathbb{C}[x,y]^{G_1}$. By the work of Shephard–Todd we know that $\mathbb{C}[x,y]^{G_1}$ is generated by $W_{e_8}(x,y)$ and the polynomial $x^4y^4(x^4-y^4)^4$. By noting

$$x^4y^4(x^4-y^4)^4=\{(W_{e_8}(x,y))^3-W_{\mathscr{G}_{24}}(x,y)\}/42,$$

we see that $\mathscr{W}[x,y]=\mathbb{C}[x,y]^{G_1}$.

Eq. (2) is rewritten as

$$Jac(\mathbf{C},\mathbf{v};x,y,u,v)=Jac\left(\mathbf{C},\mathbf{v};\frac{x+y}{\sqrt{2}},\frac{x-y}{\sqrt{2}},\frac{u+v}{\sqrt{2}},\frac{u-v}{\sqrt{2}}\right). \tag{6}$$

Since $\mathbf{C}$ is doubly even, each codeword $\mathbf{u}$ of $\mathbf{C}$ has weight divisible by 4, and we get (cf. [21])

$$Jac(\mathbf{C},\mathbf{v};x,\mathrm{i}y,u,\mathrm{i}v)=Jac(\mathbf{C},\mathbf{v};x,y,u,v). \tag{7}$$

We denote by $diag(G_1,G_1)$ the group of linear transformations generated by

$$\tilde{\sigma}_1=\begin{pmatrix}\sigma_1 & O\\ O & \sigma_1\end{pmatrix} \quad\text{and}\quad \tilde{\sigma}_2=\begin{pmatrix}\sigma_2 & O\\ O & \sigma_2\end{pmatrix}.$$

Then Eqs. (6) and (7) show that the polynomial $Jac(\mathbf{C},\mathbf{v};x,y,u,v)$ for doubly even self-dual binary code $\mathbf{C}$ is a polynomial in the ring $\mathbb{C}[x,y,u,v]^{diag(G_1,G_1)}$ of simultaneous polynomial invariants for the group G_1 in the sense of Schur [25, pp. 9–14].

3.3. Formal Jacobi polynomials

Let G_1 be the finite group introduced in the preceding subsection. A formal weight enumerator is a relative polynomial invariant of G_1 associated with the character χ of G_1, which is defined by $\chi(\sigma_1)=-1$ and $\chi(\sigma_2)=1$. Let H_1 be a subgroup of G_1 of index 2, which is the kernel of χ. H_1 is a finite unitary reflection group (No. 8 in the Shephard–Todd's list [26]) of order 96. The ring of absolute invariant polynomials for H_1 is denoted by $\mathbb{C}[x,y]^{H_1}$. The ring $\mathbb{C}[x,y]^{H_1}$ is generated by $W_{e_8}(x,y)$ and $\mathscr{E}_{12}(x,y)=x^{12}-33x^8y^4-33x^4y^8+y^{12}$ (cf. [26]).

Let $diag(H_1,H_1)$ be the matrix group defined in a similar way to $diag(G_1,G_1)$; then the invarint ring $\mathbb{C}[x,y,u,v]^{diag(H_1,H_1)}=\mathscr{R}$ (say) is the ring of simultaneous invariant polynomials for H_1.

For instance,

$$\mathscr{E}_{12,1}(x,y,u,v)=x^{11}u-11x^8y^3v-22x^7y^4u-22x^4y^7v-11x^3y^8u+y^{11}v$$

belongs to $\mathbb{C}[x,y,u,v]^{diag(H_1,H_1)}$. In [21] we called this type of polynomials as formal Jacobi polynomials. It holds that

$$\mathbb{C}[x,y,u,v]^{diag(H_1,H_1)} \supset \mathbb{C}[x,y,u,v]^{diag(G_1,G_1)}.$$

It should be noted that the dehomogenization of the ring $\mathbb{C}[x,y,u,v]^{diag(G_1,G_1)}$ is easily proved to be the ring $\mathbb{J}[X,Z]$. We denote by $\mathbb{FJ}[X,Z]$ the dehomogenization of the ring $\mathscr{R}=\mathbb{C}[x,y,u,v]^{diag(H_1,H_1)}$.

We decompose this ring $\mathscr{R}$ into a direct sum:

$$\mathscr{R}=\bigoplus_{n\geqslant 0}\mathscr{R}_n, \tag{8}$$

where $\mathscr{R}_n$ is the nth homogeneous part of $\mathscr{R}$. Further we decompose $\mathscr{R}_n$ as

$$\mathscr{R}_n=\bigoplus_{0\leqslant m\leqslant n}\mathscr{R}_{n,m}, \tag{9}$$

where $\mathscr{R}_{n,m}$ is the set of polynomials $f(x,y,u,v)\in\mathscr{R}_n$ with partial degree with respect to u and v equal to m. This set $\mathscr{R}_{n,m}$forms a vector subspace of $\mathscr{R}$. The series

$$\sum_{n\geqslant 0}\dim_{\mathbb{C}}(\mathscr{R}_n)t^n$$

is calculated by us [3]):

$$\begin{aligned}\Phi_{diag(H_1,H_1)}(t)&=\sum_{n\geqslant 0}\dim_{\mathbb{C}}(\mathscr{R}_n)t^n\\&=\frac{1+8t^8+18t^{12}+21t^{16}+19t^{20}+21t^{24}+7t^{28}+t^{32}}{(1-t^8)^2(1-t^{12})^2}\\&=1+10t^8+20t^{12}+40t^{16}+75t^{20}+130t^{24}\\&\quad+179t^{28}+283t^{32}+383t^{36}+513t^{40}\\&\quad+678t^{44}+883t^{48}+1078t^{52}+1372t^{56}\\&\quad+1658t^{60}+1994t^{64}+2385t^{68}+2836t^{72}+\cdots.\end{aligned}$$

At present we know in principle the basis of each space $\mathscr{R}_{n,m}$. Moreover we know [20, 4]

$$\sum_{n,m}\dim(\mathscr{R}_{n,m})\lambda^n\mu^m=\frac{T}{(1-\lambda^8)(1-\lambda^{12})(1-\mu^8\lambda^8)(1-\mu^{12}\lambda^{12})},$$

where

$$\begin{aligned}T&=1+\lambda^8(\mu+\mu^2+\mu^3+2\mu^4+\mu^5+\mu^6+\mu^7)+\lambda^{12}(\mu+\mu^2+2\mu^3\\&\quad+2\mu^4+2\mu^5+2\mu^6+2\mu^7+2\mu^8+2\mu^9+\mu^{10}+\mu^{11})\\&\quad+\lambda^{16}(\mu^2+\mu^3+\mu^4+2\mu^5+2\mu^6+2\mu^7+3\mu^8+2\mu^9+2\mu^{10}+2\mu^{11}\end{aligned}$$

$$+\mu^{12}+\mu^{13}+\mu^{14})+\lambda^{20}(\mu^5+\mu^6+2\mu^7+2\mu^8+2\mu^9+3\mu^{10}$$
$$+2\mu^{11}+2\mu^{12}+2\mu^{13}+\mu^{14}+\mu^{15})+\lambda^{24}(\mu^6+\mu^7+\mu^8$$
$$+2\mu^9+2\mu^{10}+2\mu^{11}+3\mu^{12}+2\mu^{13}+2\mu^{14}+2\mu^{15}+\mu^{16}+\mu^{17}+\mu^{18})$$
$$+\lambda^{28}(\mu^{11}+\mu^{12}+\mu^{13}+\mu^{14}+\mu^{15}+\mu^{16}+\mu^{17})+\lambda^{32}\mu^{16}.$$

All polynomials implied in T are explicitly determinable. For instance,

$x^8+14x^4y^4+y^8$ corresponds to λ^8,
$x^{12}-33x^8y^4-33x^4y^8+y^{12}$ corresponds to λ^{12},
$u^8+14u^4v^4+v^8$ corresponds to $\lambda^8\mu^8$,
$u^{12}-33u^8v^4-33u^4v^8+v^{12}$ corresponds to $\mu^{12}\lambda^{12}$

in the denominator and $u(x^7+7x^3y^4)+v(7x^4y^3+y^7)$ corresponds to $\lambda^8\mu$ in the numerator and so on.

4. Some facts on the spaces of Jacobi polynomials

According to the decompositions of $\mathscr{R}$ and $\mathscr{R}_n$, we can decompose the corresponding inhomogeneous counterparts $\mathbb{FJ}[X,Z]$ and $\mathbb{FJ}_n[X,Z]$ (the set of polynomials in $\mathbb{FJ}[X,Z]$ of degree n with respect to X). We can prove that if $n\equiv 0 \bmod 8$ then $\mathbb{FJ}_n[X,Z]=\mathbb{J}_n[X,Z]$ ($\mathbb{J}_n[X,Z]$ is the linear subspace of $\mathbb{J}[X,Z]$ spanned by Jacobi polynomials associated with doubly even binary codes of length n).

A powerful tool for the investigation of the simultaneous invariants of a group is the Aronhold operator (polarization) $\partial_A f(x,y,u,v)$ which is defined by (cf. [25, pp. 11–12])

$$\partial_A f(x,y,u,v)=u\frac{\partial f}{\partial x}+v\frac{\partial f}{\partial x}.$$

Proposition 6 (Schur [25]). *Suppose* $f(x,y,u,v)\in\mathscr{R}$, *then* $\partial_A f(x,y,u,v)\in\mathscr{R}$.

Definition. When $f(x,y,u,v)\in\mathscr{R}_{n,m}$, we say f has the index m.

An effect of $\partial_A:\partial_A$ does not change the total degree of $f(x,y,u,v)$, but ∂_A raises the index of $f(x,y,u,v)$ by 1.

Here *deh* is the dehomogenization map (3).

A multiple Aronhold operator ∂_A^n is inductively defined by $\partial_A^{n+1}(f)=\partial_A(\partial_A^n(f))$. $\hat{f}$ is the change of variables map $f(x,y,u,v)\to f(u,v,x,y)$.

We introduce some polynomials which belong to $\mathbb{FJ}_n[X,Z]$ for some n:

$$\lambda=xy(x^4-y^4),\quad v=xv-yu,\quad \Delta_{24}=deh(\lambda^4)=x^4(1-x^4)^4,$$
$$\zeta_0=W_{e_8}(x,y),\quad \alpha_0=deh(\zeta_0),\quad \zeta_1=\tfrac{1}{8}\partial_A(\zeta_0),\quad \alpha_1=deh(\zeta_1),$$

$$\zeta_2=\tfrac{1}{7}\partial_A(\zeta_1),\quad \alpha_2=deh(\zeta_2),\quad \zeta_3=\tfrac{1}{6}\partial_A(\zeta_2),\quad \alpha_3=deh(\zeta_3),$$

$$\alpha_{4,2}=deh(v^4),\quad \alpha_{4,1}=deh(\tfrac{1}{5}\partial_A(\zeta_3)-\tfrac{4}{5}v^4),$$

$$\alpha_5=deh(\hat{\zeta}_3),\quad \alpha_6=deh(\hat{\zeta}_2),\quad \alpha_7=deh(\hat{\zeta}_1),\quad \alpha_8=deh(\hat{\zeta}_0),$$

$$\eta_0=x^{12}-33x^8y^4-33x^4y^8+y^{12},\quad \beta_0=deh(\eta_0),\quad \eta_1=\tfrac{1}{12}\partial_A(\eta_0),\quad \beta_1=deh(\eta_1),$$

$$\eta_2=\tfrac{1}{11}\partial_A(\eta_1),\quad \beta_2=deh(\eta_2),\quad \eta_3=\partial_A(\eta_2),$$

$$\xi_3=(xv-uy)^3xy(x^4-y^4),\quad \beta_{3,2}=deh(\xi_3),$$

$$\omega_3=\tfrac{1}{10}\partial_A(\eta_2)-\tfrac{12}{5}\xi_3,\quad \beta_{3,1}=deh(\omega_3),$$

$$\xi_4=\partial_A(\xi_3),\quad \beta_{4,2}=deh(\xi_4),\quad \omega_4=\tfrac{1}{9}\partial_A(\omega_3)-\tfrac{2}{3}\xi_4,\quad \beta_{4,1}=deh(\omega_4),$$

$$\xi_5=\tfrac{1}{10}\partial_A(\xi_4),\quad \beta_{5,2}=deh(\xi_5),$$

$$\omega_5=\tfrac{1}{8}\partial_A(\omega_4)+\tfrac{1}{2}\xi_5,\quad \beta_{5,1}=deh(\omega_5),$$

$$\xi_6=\tfrac{1}{6}\partial_A(\xi_5),\quad \beta_{6,2}=deh(\xi_6),$$

$$\omega_6=\tfrac{1}{7}\partial_A(\omega_5)+\tfrac{4}{7}\xi_6,\quad \beta_{6,1}=deh(\omega_6),$$

$$\beta_{7,1}=deh(\hat{\omega}_5),\quad \beta_{7,2}=deh(\hat{\xi}_5),\quad \beta_{8,1}=deh(\hat{\omega}_4),\quad \beta_{8,2}=deh(\hat{\xi}_4),$$

$$\psi_{16,2}=deh(v^2\lambda^2),\quad \psi_{16,3}=deh(\tfrac{1}{2}\partial_A(v^2\lambda^2)),$$

$$\psi_{16,4}=deh(\tfrac{1}{2}\partial_A^2(v^2\lambda^2)),\quad \psi_{16,5,1}=deh(\tfrac{1}{60}\partial_A^3(v^2\lambda^2)),$$

$$\psi_{16,5,2}=deh(v^4)\alpha_1,\quad \psi_{16,6,1}=deh(\tfrac{1}{360}\partial_A^4(v^2\lambda^2)),$$

$$\psi_{16,6,2}=deh(v^4)\alpha_2,\quad \psi_{16,7,1}=deh(\tfrac{1}{1440}\partial_A^5(v^2\lambda^2)),$$

$$\psi_{16,7,2}=deh(v^4)\alpha_3,\quad \psi_{16,8,1}=deh(\tfrac{1}{1440}\partial_A^6(v^2\lambda^2)),$$

$$\psi_{16,8,2}=deh(v^4)\alpha_{4,1},\quad \psi_{16,8,3}=deh(v^8),$$

$$\psi_{20,5}=deh(v^4)\beta_1,\quad \psi_{20,6}=deh(v^4)\beta_2,$$

$$\psi_{20,7,1}=deh(v^4)\beta_{3,1},\quad \psi_{20,7,2}=deh(v^7\lambda),$$

$$\psi_{20,8,1}=deh(v^4)\beta_{4,1},\quad \psi_{20,8,2}=deh(\partial_A(v^7\lambda)),$$

$$\psi_{24,6}=deh(v^6\lambda^2),\quad \psi_{24,7}=deh(\tfrac{1}{2}\partial_A(v^6\lambda^2)),$$

$$\psi_{24,8}=deh(\tfrac{1}{2}\partial_A^2(v^6\lambda^2)).$$

We summarize the results for the basis of $\mathbb{F}\mathbb{J}_{40,m}[X,Z]$ $(0\leqslant m\leqslant 8)$, which is the dehomogenization of $\mathscr{R}_{40,m}$, as a proposition:

Proposition 7. *The space* $\mathbb{F}\mathbb{J}_{40,m}[X,Z]$ $(0\leqslant m\leqslant 8)$ *has basis which is given in Table* 1.

Table 1
Basis for $\mathbb{FJ}_{40,m}[X,Z]$ $(0 \leqslant m \leqslant 8)$

m						
0	α_0^5	$\alpha_0^2\Delta_{24}$				
1	$\alpha_1\alpha_0^4$	$\alpha_1\alpha_0\Delta_{24}$	$\beta_1\beta_0\alpha_0^2$			
2	$\alpha_2\alpha_0^4$	$\alpha_2\alpha_0\Delta_{24}$	$\beta_2\beta_0\alpha_0^2$	$\psi_{16,2}\alpha_0^3$	$\psi_{16,2}\Delta_{24}$	
3	$\alpha_3\alpha_0^4$	$\alpha_3\alpha_0\Delta_{24}$	$\beta_{3,1}\beta_0\alpha_0^2$	$\beta_{3,2}\beta_0\alpha_0^2$	$\psi_{16,3}\alpha_0^3$	$\psi_{16,3}\Delta_{24}$
4	$\alpha_{4,1}\alpha_0^4$	$\alpha_{4,1}\alpha_0\Delta_{24}$	$\alpha_{4,2}\alpha_0^4$	$\alpha_{4,2}\alpha_0\Delta_{24}$	$\beta_{4,1}\beta_0\alpha_0^2$	$\beta_{4,2}\beta_0\alpha_0^2$
	$\psi_{16,4}\alpha_0^3$	$\psi_{16,4}\Delta_{24}$				
5	$\alpha_5\alpha_0^4$	$\alpha_5\alpha_0\Delta_{24}$	$\beta_{5,1}\beta_0\alpha_0^2$	$\beta_{5,2}\beta_0\alpha_0^2$	$\psi_{16,5,1}\alpha_0^3$	$\psi_{16,5,1}\Delta_{24}$
	$\psi_{16,5,2}\alpha_0^3$	$\psi_{16,5,2}\Delta_{24}$	$\psi_{20,5}\beta_0\alpha_0$			
6	$\alpha_6\alpha_0^4$	$\alpha_6\alpha_0\Delta_{24}$	$\beta_{6,1}\beta_0\alpha_0^2$	$\beta_{6,2}\beta_0\alpha_0^2$	$\psi_{16,6,1}\alpha_0^3$	$\psi_{16,6,1}\Delta_{24}$
	$\psi_{16,6,2}\alpha_0^3$	$\psi_{16,6,2}\Delta_{24}$	$\psi_{20,6}\beta_0\alpha_0$	$\psi_{24,6}\alpha_0^2$		
7	$\alpha_7\alpha_0^4$	$\alpha_7\alpha_0\Delta_{24}$	$\beta_{7,1}\beta_0\alpha_0^2$	$\beta_{7,2}\beta_0\alpha_0^2$	$\psi_{16,7,1}\alpha_0^3$	$\psi_{16,7,1}\Delta_{24}$
	$\psi_{16,7,2}\alpha_0^3$	$\psi_{16,7,2}\Delta_{24}$	$\psi_{20,7,1}\beta_0\alpha_0$	$\psi_{20,7,2}\beta_0\alpha_0$	$\psi_{24,7}\alpha_0^2$	
8	$\alpha_8\alpha_0^4$	$\alpha_8\alpha_0\Delta_{24}$	$\beta_{8,1}\beta_0\alpha_0^2$	$\beta_{8,2}\beta_0\alpha_0^2$	$\psi_{16,8,1}\alpha_0^3$	$\psi_{16,8,1}\Delta_{24}$
	$\psi_{16,8,2}\alpha_0^3$	$\psi_{16,8,2}\Delta_{24}$	$\psi_{16,8,3}\alpha_0^3$	$\psi_{16,8,3}\Delta_{24}$	$\psi_{20,8,1}\beta_0\alpha_0$	$\psi_{20,8,2}\beta_0\alpha_0$
	$\psi_{24,8}\alpha_0^2$					

5. Relation between covering radius of codes and Jacobi polynomials

Our key theorem is

Theorem 5. *Let* $\mathbf{C}$ *be a self-dual binary code of length n. We take any vector* $\mathbf{v}$ *in* $\mathbf{F}_2^n$. *If* U *is the coset in* $\mathbf{F}_2^n/\mathbf{C}$ *to which* $\mathbf{v}$ *belongs, then we have*

$$W_U(X) = X^{wt(\mathbf{v})} Jac(C, \mathbf{v} \mid X, X^{-2}),$$

where $Jac(C, \mathbf{v} \mid X, Z)$ *is the Jacobi polynomial for the code* $\mathbf{C}$ *with respect to* $\mathbf{v}$.

Proof. We put $wt(\mathbf{v}) = k$. From the defining equation of $Jac(C, \mathbf{v} \mid X, Z)$ we have

$$\begin{aligned} X^k Jac(C, \mathbf{v} \mid X, X^{-2}) &= \sum_{\mathbf{x}\in\mathbf{C}} X^{wt(\mathbf{x})+wt(\mathbf{v})-2\mathbf{x}*\mathbf{v}} \\ &= \sum_{\mathbf{x}\in\mathbf{C}} X^{wt(\mathbf{x}+\mathbf{v})} \\ &= \sum_{\mathbf{u}\in\mathbf{C}+\mathbf{v}} X^{wt(\mathbf{u})} \\ &= W_U(X). \end{aligned}$$

From this theorem, we can show a functional equation of $W_U(X)$:

$$X^{wt(\mathbf{v})} Jac(C, \mathbf{v} \mid X, X^{-2}) = \frac{1}{|\mathbf{C}|}(1+X)^n Jac\left(C, \mathbf{v} \,\middle|\, \frac{1-X}{1+X}, (-1)\right)$$

Example. For the Hamming code e_8 and a vector $\mathbf{v}$ of weight 1,

$$Jac(e_8, \mathbf{v} \mid X, Z) = 1 + X^4(7Z+7) + X^8 Z.$$

Therefore we get

$$\begin{aligned} W_U(X) &= X\{1 + X^4(7X^{-2} + 7) + X^8X^{-2}\} \\ &= X + 7X^3 + 7X^5 + X^7 \\ &= \frac{1}{2^4}(1+X)^8\left[1 - \left(\frac{1-X}{1+X}\right)^8\right]. \end{aligned}$$

As an application of the Theorem 5, we can determine covering radii of the extremal binary self-dual codes of lengths 40 and 56. We expect that good informations on non-extremal codes are obtainable.

We now give a precise information on the relation between the multiplicity of Jacobi polynomials and the multiplicity of the coset weight enumerators. To do this we need a definition.

Definition. Let $\mathbf{C}$ be a binary code of length n. Let $\mathbf{v}$ be a vector in $\mathbf{F}_2^n$. The vector $\mathbf{v}$ is called rigid (with respect to $\mathbf{C}$) if $wt(\mathbf{v})$ is minimal in its coset $\mathbf{v}+\mathbf{C}$ i.e. if $\mathbf{v}$ satisfies

$$wt(\mathbf{v}) = \min_{\mathbf{x}\in\mathbf{v}+\mathbf{C}} wt(\mathbf{x}).$$

Usually a rigid vector $\mathbf{v}$ is called a coset leader of the coset $\mathbf{v}+\mathbf{C}$. A vector $\mathbf{v}$ in $\mathbf{F}_2^n$ is fragile (with respect to $\mathbf{C}$) if $\mathbf{v}$ is not rigid. A Jacobi polynomial $Jac(\mathbf{C},\mathbf{v}\,|\,X,Z)$ is rigid if $\mathbf{v}$ is rigid and fragile if $\mathbf{v}$ is fragile. Note that if the vector $\mathbf{v}$ is fragile then the coset weight enumerator $W_{\mathbf{v}+\mathbf{C}}(X) = X^{wt(\mathbf{v})}Jac(C,\mathbf{v}\,|\,X,X^{-2})$ of $\mathbf{v}+\mathbf{C}$ contains non-vanishing term a_hX^h with $h<k$.

Proposition 8. *Assume that* $(*)$ *in a binary linear code* $\mathbf{C}$ *any two different rigid Jacobi polynomials derive* (*via the process in Theorem* 5) *different coset weight enumerators. Then the coset leaders* $\mathbf{v}_1,\mathbf{v}_2$ *of the same coset have identical Jacobi polynomial.*

Proof. Suppose two coset leaders $\mathbf{v}_1$ and $\mathbf{v}_2$ in a coset have two different Jacobi polynomials $Jac(\mathbf{C},\mathbf{v}_1\,|\,X,Z)$ and $Jac(\mathbf{C},\mathbf{v}_2\,|\,X,Z)$ respectively. By the definition of coset leader, we have $wt(\mathbf{v}_1) = wt(\mathbf{v}_2) = k$ (say). It is obvious that these two coset leaders $\mathbf{v}_1$ and $\mathbf{v}_2$ induce the same coset distribution. This implies that

$$W_{\mathbf{v}_1+\mathbf{C}}(X) = W_{\mathbf{v}_2+\mathbf{C}}(X).$$

By Theorem 5 we have

$$\begin{aligned} W_{\mathbf{v}_1+\mathbf{C}}(X) &= X^k Jac(\mathbf{C},\mathbf{v}_1\,|\,X,X^{-2}), \\ W_{\mathbf{v}_2+\mathbf{C}}(X) &= X^k Jac(\mathbf{C},\mathbf{v}_2\,|\,X,X^{-2}). \end{aligned}$$

But this contradicts to the assumption $(*)$. Thus we can conclude that

$$Jac(\mathbf{C},\mathbf{v}_1\,|\,X,Z) = Jac(\mathbf{C},\mathbf{v}_2\,|\,X,Z). \qquad \square$$

Theorem 6. *Let* $\mathbf{C}$ *be a binary code of length n. We are under the same assumption* $(*)$ *as in Proposition* 8. *Let* $\mathbf{R}_k$ *be the set of rigid vectors of a fixed weight k with equal rigid Jacobi polynomials* $Jac(\mathbf{C},\mathbf{v}\,|\,X,Z)$. *Let*

$$\begin{aligned} &X^k Jac(\mathbf{C},\mathbf{v}\,|\,X,X^{-2}) \\ &\quad = W_{\mathbf{v}+\mathbf{C}}(X) \\ &\quad = a_k X^k + a_{k+1}X^{k+1} + \cdots \end{aligned} \tag{10}$$

be its common coset weight enumerator, then the number of the different cosets $\mathbf{S}$ *in* $\mathbf{F}_2^n/\mathbf{C}$ *such that*

$$W_{\mathbf{S}}(X) = W_{\mathbf{v}+\mathbf{C}}(X)$$

is given by $|\mathbf{R}_k|/a_k$.

Proof. Proof of Theorem. By Proposition 8, a_k rigid vectors $\mathbf{v}_i$ $(1 \leqslant i \leqslant a_k)$ have identical Jacobi polynomial. Let $\mathscr{S}$ be the set consisting of all cosets $\mathbf{S}$ such that the weight of $\mathbf{S}$ (i.e. the weight of the coset leader) is k and $W_{\mathbf{S}}(X) = W_{\mathbf{v}_i+\mathbf{C}}(X)$. We show that the map

$$\begin{array}{ccc} \phi : \mathbf{R}_k & \to & \mathscr{S} \\ \bigcup & & \bigcup \\ \mathbf{v} & \mapsto & \mathbf{v}+\mathbf{C} \end{array}$$

is an a_k-to-one correspondence. Let $\mathbf{v} \in \mathbf{R}_k$. By (10) there are exactly a_k rigid vectors $\mathbf{v}_i$ $(1 \leqslant i \leqslant a_k,\ \mathbf{v}_1 = \mathbf{v})$. They are congruent to $\mathbf{v}$ modulo $\mathbf{C}$, and only they go into the same $\mathbf{S}$ in $\mathscr{S}$ by the map ϕ. Therefore, among vectors in $\mathbf{R}_k$ only a_k vectors belong to the same coset. Thus, the number of different cosets $\mathbf{S}$ in $\mathrm{F}_2^n/\mathbf{C}$ with $W_{\mathbf{S}}(X) = W_{\mathbf{v}+\mathbf{C}}(X)$ is $|\mathbf{R}_k|/a_k$. □

There are cases where Theorem 6 fails in its efficiency. In fact, for some cosets of weights $\geqslant 4$ in certain extremal binary $[40, 20, 8]$ codes it happens that two rigid vectors (i.e. coset leaders) $\mathbf{v}_1$ and $\mathbf{v}_2$ in the same coset $\mathbf{S}$ induces different Jacobi polynomials $Jac(\mathbf{C},\mathbf{v}_1\,|\,X,Z)$ and $Jac(\mathbf{C},\mathbf{v}_2\,|\,X,Z)$. So they slip away the assumption $(*)$. For this case one must prepare a weaker statement than Theorem 6.

Let $\mathbf{C}$ be a binary code of length n. Let $\mathbf{v}$ be a coset leader of weight k of a coset $\mathbf{S} \in \mathbf{F}_2^n/\mathbf{C}$, and $Jac(\mathbf{C},\mathbf{v}\,|\,X,Z)$ be Jacobi polynomial associated with $\mathbf{v}$. It holds that

$$W_{\mathbf{S}}(X) = X^{wt(\mathbf{v})} Jac(\mathbf{C},\mathbf{v}\,|\,X,X^{-2}).$$

Let $T_k(W_{\mathbf{S}}(X))$ be the set of all rigid vectors $\mathbf{u}$ of weight k in $\mathbf{F}_2^n$ such that

$$\begin{aligned} W_{\mathbf{u}+\mathbf{C}}(X) &= W_{\mathbf{S}}(X) \\ &= b_k X^k + \cdots \end{aligned}$$

holds.

Theorem 7. *Let the notations be as above. Then the number* α *of different cosets* $\overline{\mathbf{S}}$ *of weight* k *with the same coset weight distribution described by* $W_{\mathbf{S}}(X)$ *is given by*

$$\alpha = \frac{|T_k(W_{\mathbf{S}}(X)|}{b_k}.$$

The proof of this statement is quite similar to that of Theorem 6 and hence we omit it. The following proposition is of practical use if we want to determine rigid Jacobi polynomials or covering radius of codes.

Proposition 9. *Let*

$$Jac(\mathbf{C}, \mathbf{v} \mid X, Z) = \sum_{m=0}^{n} \sum_{r=0}^{k} b(m,r) X^m Z^r \ \textit{with}\ wt(\mathbf{v}) = k$$

be a Jacobi polynomial for a code $\mathbf{C}$*. It is rigid if and only if*

$$b(m,r) = 0$$

holds for $m < 2r$.

Proof. Let $\mathbf{v} + \mathbf{C}$ be the coset to which $\mathbf{v}$ belongs. By Theorem 4 the coset weight enumerator $W_{\mathbf{v}+\mathbf{C}}(X)$ is given by

$$\begin{aligned} W_{\mathbf{v}+\mathbf{C}}(X) &= X^k Jac(\mathbf{C}, \mathbf{v} \mid X, X^{-2}) \\ &= X^k \sum_{m=0}^{n} \sum_{r=0}^{k} b(m,r) X^m X^{-2r} \\ &= \sum_{m=0}^{n} \sum_{r=0}^{k} b(m,r) X^{m+k-2r}. \end{aligned}$$

If there exists a pair of m and r such that $b(m,r) \neq 0$ with $m + k - 2r < k$, then this implies that the coset $\mathbf{v} + \mathbf{C}$ contains a vector $\mathbf{u}$ with $wt(\mathbf{u}) < k$. In that case the vector $\mathbf{v}$ is not a coset leader of the coset $\mathbf{v} + \mathbf{C}$. Conversely if $b(m,r) = 0$ holds for $m < 2r$, then by the equations above there does not exist any vector $\mathbf{u}$ with $wt(\mathbf{u}) < k$, and $\mathbf{v}$ is a coset leader of the coset $\mathbf{v} + \mathbf{C}$. This completes the proof of the proposition.

6. Linear subspaces of Jacobi polynomials

Up to now we have treated general Jacobi polynomials or formal Jacobi polynomials connected with doubly even codes $\mathbf{C}$. Since we are exclusively interested in extremal $[40, 20, 8]$ binary codes, from here we consider the linear subspace $\mathbb{J}_{40,m}(ext)[X, Z]$ spanned by Jacobi polynomials of index m for such codes. Further, for covering radius problem, we have only to consider the linear subspace $\mathbb{J}_{40,m}(ext, rigid)[X, Z]$ of $\mathbb{J}_{40,m}(ext)[X, Z]$ spanned by rigid Jacobi polynomials of index m for extremal codes. By using a computer algebra system [5] from the linear basis for $\mathbb{F}\mathbb{J}_{40,m}[X, Z]$ $(0 \leqslant m \leqslant 8)$

Table 2

m	0	1	2	3	4	5	6	7	8
s_m	2	3	5	6	8	9	10	11	13
t_m	1	1	2	2	3	4	5	6	8
u_m	1	1	2	2	3	3	3	2	2

given in Proposition 7 we can cut out linear basis of $\mathbb{J}_{40,m}(ext)[X,Z]$ and $\mathbb{FJ}_{40,m}[X,Z]$, respectively. First let $s_m = \dim \mathbb{J}_{40,m}[X,Z]$, $t_m = \dim \mathbb{FJ}_{40,m}(ext)[X,Z]$ and $u_m = \dim \mathbb{FJ}_{40,m}(ext, rigid)[X,Z]$. We give these values in Table 2.

Here we give a basis of each $\mathbb{FJ}_{40,m}(ext, rigid)[X,Z]$ $(1 \leqslant m \leqslant 8)$. As a abbreviation we use the notation $\mathscr{REJ}_{40,m} = \mathbb{FJ}_{40,m}(ext, rigid)[X,Z]$. We remark that dots parts are easily recovered from the preceding terms in viewing Proposition 4.

Since the process described in Theorem 5 is algebraic in nature, it can be extended to any element of $\mathscr{REJ}_{40,m}$ $(m \geqslant 0)$, and we denote this mapping by φ_m $(m = wt(\mathbf{v}))$.

Fact 1. *$\mathscr{REJ}_{40,1}$ has a base*

$$\begin{aligned} f_{40,1} &= \tfrac{11}{18}\alpha_1\alpha_0^4 - 28\alpha_1\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_1\beta_0\alpha_0^2 \\ &= 1 + (57Z + 228)X^8 + (6384Z + 14896)X^{12} + (95988Z + 143982)X^{16} \\ &\quad + (262752Z + 262752)X^{20} + \cdots . \end{aligned}$$

Fact 2. *$\mathscr{REJ}_{40,2}$ has basis*:

$$\begin{aligned} f_{40,2}^{(1)} &= \psi_{16,2}\Delta_{24} \\ &= (Z^2 - 2Z + 1)X^8 + (-6Z^2 + 12Z - 6)X^{12} + (15Z^2 - 30Z + 15)X^{16} \\ &\quad + (-20Z^2 + 40Z - 20)X^{20} + \cdots, \\ f_{40,2}^{(2)} &= \tfrac{11}{18}\alpha_2\alpha_0^4 - 28\alpha_2\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_2\beta_0\alpha_0^2 - \tfrac{2}{3}\psi_{16,2}\alpha_0^3 + 7\psi_{16,2}\Delta_{24} \\ &= 1 + (114Z + 171)X^8 + (1862Z^2 + 9044Z + 10374)X^{12} + (36765Z^2 \\ &\quad + 118446Z + 84759)X^{16} + +(128212Z^2 + 269080Z + 128212)X^{20} + \cdots . \end{aligned}$$

Fact 3. *$\mathscr{REJ}_{40,3}$ has basis*:

$$\begin{aligned} f_{40,3}^{(1)} &= \psi_{16,3}\Delta_{24} \\ &= (Z^3+3Z^2-9Z+5)X^8+(-10Z^3-6Z^2+42Z-26)X^{12} \\ &\quad + (35Z^3-15Z^2-75Z+55)X^{16}+(-60Z^3+60Z^2+60Z-60)X^{20}+\cdots, \\ f_{40,3}^{(2)} &= \tfrac{11}{18}\alpha_3\alpha_0^4-28\alpha_3\alpha_0\Delta_{24}+\tfrac{7}{18}\beta_{3,1}\beta_0\alpha_0^2+\tfrac{8}{9}\beta_{3,2}\beta_0\alpha_0^2-\tfrac{1}{3}\psi_{16,3}\alpha_0^3+7\psi_{16,3}\Delta_{24} \\ &= 1+(21Z^2+129Z+135)X^8+(490Z^3+3990Z^2+9702Z+7098)X^{12} \\ &\quad + (13545Z^3+69975Z^2+107379Z+49071)X^{16} \\ &\quad + (60732Z^3+202020Z^2+202020Z+60732)X^{20}+\cdots . \end{aligned}$$

Fact 4. *$\mathscr{REJ}_{40,4}$ has basis*:

$$\begin{aligned}
f_{40,4}^{(1)} &= -\tfrac{1}{22}\alpha_{4,2}\alpha_0\Delta_{24} + \tfrac{1}{22}\psi_{16,4}\Delta_{24}\\
&= (Z^3 - 3Z + 2)X^8 + (-2Z^4 - 2Z^3 + 14Z - 10)X^{12}\\
&\quad + (10Z^4 - 5Z^3 - 25Z + 20)X^{16} + (-20Z^4 + 20Z^3 + 20Z - 20)X^{20} + \cdots,\\
f_{40,4}^{(2)} &= \tfrac{9}{11}\alpha_{4,2}\alpha_0\Delta_{24} + \tfrac{2}{11}\psi_{16,4}\Delta_{24}\\
&= (Z^4 + 6Z^2 - 16Z + 9)X^8 + (2Z^4 - 48Z^3 + 60Z^2 + 16Z - 30)X^{12}\\
&\quad + (-9Z^4 + 176Z^3 - 294Z^2 + 96Z + 31)X^{16}\\
&\quad + (-4Z^4 - 224Z^3 + 456Z^2 - 224Z - 4)X^{20} + \cdots,\\
f_{40,4}^{(3)} &= \tfrac{11}{18}\alpha_{4,1}\alpha_0^4 - 28\alpha_{4,1}\alpha_0\Delta_{24} - \tfrac{49}{99}\alpha_{4,1}\alpha_0^4 + \tfrac{239}{11}\alpha_{4,2}\alpha_0\Delta_{24}\\
&\quad + \tfrac{7}{18}\beta_{4,1}\beta_0\alpha_0^2 + \tfrac{1}{3}\beta_{4,2}\beta_0\alpha_0^2 - \tfrac{2}{33}\psi_{16,4}\alpha_0^3 + \tfrac{14}{11}\psi_{16,4}\Delta_{24}\\
&= 1 + (42Z^2 + 144Z + 99)X^8 + (126Z^4 + 1456Z^3 + 5796Z^2 + 9072Z\\
&\quad + 4830)X^{12} + (4725Z^4 + 35280Z^3 + 87030Z^2 + 85152Z + 27783)X^{16}\\
&\quad + (27972Z^4 + 131040Z^3 + 207480Z^2 + 131040Z + 27972)X^{20} + \cdots.
\end{aligned}$$

Fact 5. *$\mathscr{REJ}_{40,5}$ has basis*:

$$\begin{aligned}
f_{40,5}^{(1)} &= \tfrac{1}{11}\psi_{16,5,1}\Delta_{24} - \tfrac{1}{11}\psi_{16,5,2}\Delta_{24}\\
&= (Z^3 - Z^2 - Z + 1)X^8 + (-Z^5 + Z^4 - 4Z^3 + 4Z^2 + 5Z - 5)X^{12}\\
&\quad + (5Z^5 - 5Z^4 + 5Z^3 - 5Z^2 - 10Z + 10)X^{16}\\
&\quad + (-10Z^5 + 10Z^4 + 10Z - 10)X^{20} + \cdots,\\
f_{40,5}^{(2)} &= \tfrac{4}{11}\psi_{16,5,1}\Delta_{24} + \tfrac{7}{11}\psi_{16,5,2}\Delta_{24}\\
&= (Z^4 + 2Z^2 - 8Z + 5)X^8 + (3Z^5 - 21Z^4 + 14Z^3 + 6Z^2 + 15Z - 17)X^{12}\\
&\quad + (-7Z^5 + 66Z^4 - 54Z^3 - 44Z^2 + 21Z + 18)X^{16}\\
&\quad + (-2Z^5 - 74Z^4 + 76Z^3 + 76Z^2 - 74Z - 2)X^{20} + \cdots,\\
f_{40,5}^{(3)} &= \tfrac{11}{18}\alpha_5\alpha_0^4 - 28\alpha_5\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_{5,1}\beta_0\alpha_0^2 + \tfrac{1}{9}\beta_{5,2}\beta_0\alpha_0^2\\
&\quad - \tfrac{10}{33}\psi_{16,5,1}\alpha_0^3 + \tfrac{70}{11}\psi_{16,5,1}\Delta_{24} - \tfrac{17}{198}\psi_{16,5,2}\alpha_0^3 + \tfrac{29}{11}\psi_{16,5,2}\Delta_{24} + \tfrac{1}{18}\psi_{20,5}\beta_0\alpha_0\\
&= 1 + (70Z^2 + 145Z + 70)X^8\\
&\quad + (35Z^5 + 455Z^4 + 2730Z^3 + 6930Z^2 + 7875Z + 3255)X^{12}\\
&\quad + (1540Z^5 + 15925Z^4 + 56350Z^3 + 88700Z^2 + 62090Z + 15365)X^{16}\\
&\quad + (12502Z^5 + 77350Z^4 + 172900Z^3 + 172900Z^2 + 77350Z + 12502)X^{20}\\
&\quad + \cdots.
\end{aligned}$$

Fact 6. *$\mathscr{REJ}_{40,6}$ has basis*:

$$\begin{aligned}
f^{(1)}_{40,6} &= \tfrac{1}{11}\psi_{16,6,1}\Delta_{24} - \tfrac{3}{11}\psi_{16,6,2}\Delta_{24}\\
&= (2Z^3 - 3Z^2 + 1)X^8 + (-Z^6 + 3Z^4 - 12Z^3 + 15Z^2 - 5)X^{12}\\
&\quad + (5Z^6 - 15Z^4 + 30Z^3 - 30Z^2 + 10)X^{16}\\
&\quad + (-10Z^6 + 30Z^4 - 40Z^3 + 30Z^2 - 10)X^{20} + \cdots,
\end{aligned}$$

$$\begin{aligned}
f^{(2)}_{40,6} &= \tfrac{2}{11}\psi_{16,6,1}\Delta_{24} + \tfrac{5}{11}\psi_{16,6,2}\Delta_{24}\\
&= (Z^4 - 4Z + 3)X^8 + (Z^6 - 4Z^5 - 9Z^4 + 16Z^3 - 5Z^2 + 12Z - 11)X^{12}\\
&\quad + (-Z^6 + 12Z^5 + 26Z^4 - 64Z^3 + 21Z^2 - 8Z + 14)X^{16}\\
&\quad + (-6Z^6 - 8Z^5 - 34Z^4 + 96Z^3 - 34Z^2 - 8Z - 6)X^{20} + \cdots,
\end{aligned}$$

$$\begin{aligned}
f^{(3)}_{40,6} &= \tfrac{11}{18}\alpha_6\alpha_0^4 - 28\alpha_6\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_{6,1}\beta_0\alpha_0^2 - \tfrac{4}{9}\beta_{6,2}\beta_0\alpha_0^2\\
&\quad - \tfrac{10}{33}\psi_{16,6,1}\alpha_0^3 + \tfrac{70}{11}\psi_{16,6,1}\Delta_{24} - \tfrac{17}{66}\psi_{16,6,2}\alpha_0^3 + \tfrac{87}{11}\psi_{16,6,2}\Delta_{24} + \tfrac{1}{6}\psi_{20,6}\beta_0\alpha_0\\
&= 1 + (105Z^2 + 132Z + 48)X^8 + (13Z^6 + 132Z^5 + 1035Z^4 + 4080Z^3\\
&\quad + 7335Z^2 + 6516Z + 2169)X^{12} + (454Z^6 + 6516Z^5 + 31485Z^4 + 70720Z^3\\
&\quad + 80010Z^2 + 42504Z + 8281)X^{16} + (5418Z^6 + 42504Z^5 + 125790Z^4\\
&\quad + 178080Z^3 + 125790Z^2 + 42504Z + 5418)X^{20} + \cdots.
\end{aligned}$$

Fact 7. *$\mathscr{REJ}_{40,7}$ has basis*:

$$\begin{aligned}
f^{(1)}_{40,7} &= \tfrac{1}{11}\psi_{16,7,1}\Delta_{24} + \tfrac{1}{11}\psi_{16,7,2}\Delta_{24}\\
&= (Z^4 + Z^3 - 3Z^2 - Z + 2)X^8 + (-Z^6 - 3Z^5 + 9Z^2 + 3Z - 8)X^{12}\\
&\quad + (2Z^7 + 3Z^6 + 9Z^5 - 9Z^4 - 9Z^3 - 6Z^2 - 2Z + 12)X^{16}\\
&\quad + (-8Z^7 - 2Z^6 - 6Z^5 + 16Z^4 + 16Z^3 - 6Z^2 - 2Z - 8)X^{20} + \cdots,
\end{aligned}$$

$$\begin{aligned}
f^{(2)}_{40,7} &= \tfrac{11}{18}\alpha_7\alpha_0^4 - 28\alpha_7\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_{7,1}\beta_0\alpha_0^2 + \tfrac{7}{9}\beta_{7,2}\beta_0\alpha_0^2 - \tfrac{7}{33}\psi_{16,7,1}\alpha_0^3\\
&\quad + 5\psi_{16,7,1}\Delta_{24} - \tfrac{119}{198}\psi_{16,7,2}\alpha_0^3 + 13\psi_{16,7,2}\Delta_{24} + \tfrac{7}{18}\psi_{20,7,1}\beta_0\alpha_0 + \tfrac{5}{9}\psi_{20,7,2}\beta_0\alpha_0\\
&= 1 + (30Z^3 + 93Z^2 + 123Z + 39)X^8 + (31Z^6 + 369Z^5 + 1860Z^4 + 5100Z^3\\
&\quad + 7389Z^2 + 5139Z + 1392)X^{12} + (145Z^7 + 2463Z^6 + 15417Z^5 + 47470Z^4\\
&\quad + 76740Z^3 + 65610Z^2 + 27718Z + 4407)X^{16} + (2208Z^7 + 21870Z^6\\
&\quad + 83154Z^5 + 155520Z^4 + 155520Z^3 + 83154Z^2 + 21870Z + 2208)X^{20}\\
&\quad + \cdots.
\end{aligned}$$

Fact 8. *$\mathscr{REJ}_{40,8}$ has basis*:

$$\begin{aligned}
f^{(1)}_{40,8} &= -\tfrac{2}{231}\psi_{16,8,1}\Delta_{24} - \tfrac{1}{11}\psi_{16,8,2}\Delta_{24} + \tfrac{19}{231}\psi_{16,8,3}\Delta_{24}\\
&= 1 + (-Z^4 + 2Z^2 - 1)X^8 + (2Z^6 - 6Z^2 + 4)X^{12}\\
&\quad + (-Z^8 - 6Z^6 + 9Z^4 + 4Z^2 - 6)X^{16} + (4Z^8 + 4Z^6 - 16Z^4 + 4Z^2 + 4)X^{20}\\
&\quad + (-6Z^8 + 4Z^6 + 9Z^4 - 6Z^2 - 1)X^{24} + (4Z^8 - 6Z^6 + 2Z^2)X^{28}\\
&\quad + (-8Z^8 + 2Z^6 - Z^4)X^{32},
\end{aligned}$$

$$\begin{aligned}
f^{(2)}_{40,8} &= \tfrac{11}{18}\alpha_8\alpha_0^4 - 28\alpha_8\alpha_0\Delta_{24} + \tfrac{7}{18}\beta_{8,1}\beta_0\alpha_0^2 + \tfrac{7}{9}\beta_{8,2}\beta_0\alpha_0^2 - \tfrac{119}{99}\psi_{16,8,2}\alpha_0^3\\
&\quad + 26\psi_{16,8,2}\Delta_{24} - \tfrac{4}{99}\psi_{16,8,1}\alpha_0^3 + \tfrac{20}{21}\psi_{16,8,1}\Delta_{24} + \tfrac{71}{99}\psi_{16,8,3}\alpha_0^3 - \tfrac{316}{21}\psi_{16,8,3}\Delta_{24}\\
&\quad + \tfrac{7}{9}\psi_{20,8,1}\beta_0\alpha_0 + \tfrac{2}{9}\psi_{20,8,2}\beta_0\alpha_0\\
&= 1 + (48Z^3 + 100Z^2 + 112Z + 25)X^8\\
&\quad + (124Z^6 + 736Z^5 + 2800Z^4 + 5920Z^3 + 6892Z^2 + 3904Z + 904)X^{12}\\
&\quad + (35Z^8 + 880Z^7 + 6772Z^6 + 27568Z^5 + 60480Z^4 + 74400Z^3\\
&\quad + 50280Z^2 + 17312Z + 2243)X^{16} + (888Z^8 + 10560Z^7 + 50520Z^6\\
&\quad + 120704Z^5 + 160160Z^4 + 120704Z^3 + 50520Z^2 + 10560Z + 888)X^{20}\\
&\quad + (2243Z^8 + 17312Z^7 + 50280Z^6 + 74400Z^5 + 60480Z^4 + 27568Z^3\\
&\quad + 6772Z^2 + 880Z + 35)X^{24} + (904Z^8 + 3904Z^7 + 6892Z^6 + 5920Z^5\\
&\quad + 2800Z^4 + 736Z^3 + 124Z^2)X^{28} + (25Z^8 + 112Z^7\\
&\quad + 100Z^6 + 48Z^5)X^{32} + Z^8X^{40}.
\end{aligned}$$

As before the weight of a coset is the weight of the coset leader of the coset. Combining Facts 1–8 with Theorem 5, we get

Proposition 10. *Let the notations be as above*; *then we have*

(1) *The coset weight enumerator of a coset of weight* 1 *equals to*

$$\begin{aligned}
\varphi_1(f_{40,1}) &= X + 57X^7 + 228X^9 + 6384X^{11} + 14896X^{13} + 95988X^{15}\\
&\quad + 143982X^{17} + 262752X^{19} + \cdots .
\end{aligned}$$

(2) *The coset weight enumerator of a coset of weight* 2 *is a linear integral combination of*

$$\begin{aligned}
\varphi_1(f^{(1)}_{40,2}) &= X^6 - 2X^8 - 5X^{10} + 12X^{12} + 9X^{14} - 30X^{16} - 5X^{18} + 40X^{20} + \cdots,\\
\varphi_2(f^{(2)}_{40,2}) &= X^2 + 114X^8 + 2033X^{10} + 9044X^{12} + 47139X^{14} + 118446X^{16}\\
&\quad + 212971X^{18} + 269080X^{20} + \cdots .
\end{aligned}$$

(3) *The coset weight enumerator of a coset of weight* 3 *is a linear integral combination of*

$$\varphi_3(f_{40,3}^{(1)}) = X^5 + 3X^7 - 19X^9 - X^{11} + 77X^{13} - 41X^{15} - 135X^{17} + 115X^{19} + \cdots$$
$$\varphi_3(f_{40,3}^{(2)}) = X^3 + 21X^7 + 619X^9 + 4125X^{11} + 23247X^{13} + 77073X^{15} + 168111X^{17} + 251091X^{19} + \cdots .$$

(4) *The coset weight enumerator of a coset of weight* 4 *is a linear integral combination of*

$$\varphi_4(f_{40,4}^{(1)}) = X^6 - 2X^8 - 5X^{10} + 12X^{12} + 9X^{14} - 30X^{16} - 5X^{18} + 40X^{20} + \cdots,$$
$$\varphi_3(f_{40,4}^{(2)}) = X^4 + 8X^8 - 64X^{10} + 60X^{12} + 192X^{14} - 328X^{16} - 128X^{18} + 518X^{20} + \cdots,$$
$$\varphi_4(f_{40,4}^{(3)}) = X^4 + 168X^8 + 1600X^{10} + 10620X^{12} + 44352X^{14} + 119832X^{16} + 216192X^{18} + 263046X^{20} + \cdots .$$

(5) *The coset weight enumerator of a coset of weight* 5 *is a linear integral combination of*

$$\varphi_5(f_{40,5}^{(2)}) = X^5 + 3X^7 - 19X^9 - X^{11} + 77X^{13} - 41X^{15} - 135X^{17} + 115X^{19} + \cdots,$$
$$\varphi_5(f_{40,5}^{(3)}) = X^5 + 35X^7 + 525X^9 + 4415X^{11} + 22925X^{13} + 76727X^{15} + 169305X^{17} + 250355X^{19} + \cdots .$$

(6) *The coset weight enumerator of a coset of weight* 6 *is a linear integral combination of*

$$\varphi_6(f_{40,6}^{(1)}) = -X^6 + 2X^8 + 5X^{10} - 12X^{12} - 9X^{14} + 30X^{16} + 5X^{18} - 40X^{20} + \cdots,$$
$$\varphi_6(f_{40,6}^{(3)}) = 14X^6 + 132X^8 + 1594X^{10} + 10728X^{12} + 44286X^{14} + 119740X^{16} + 216250X^{18} + 263088X^{20} + \cdots .$$

(7) *The coset weight enumerator of a coset of weight* 7 *equals*

$$\varphi_7(f_{40,7}^{(1)}) = 32X^7 + 544X^9 + 4416X^{11} + 22848X^{13} + 76768X^{15} + 16944X^{17} + 250240X^{19} + \cdots .$$

(8) *The coset weight enumerator of a coset of weight* 8 *equals*

$$\varphi_8(f_{40,8}^{(1)}) = 160X^8 + 1664X^{10} + 10560X^{12} + 44160X^{14} + 120160X^{16} + 216320X^{18} + 262528X^{20} + 216320X^{22} + 120160X^{24} + 44160X^{26} + 1664X^{30} + 10560X^{28} + 160X^{32}.$$

Remark 2. One sees that $\varphi_5(f^{(1)}_{40,5})=0$, $\varphi_6(f^{(2)}_{40,6})=-2\varphi_6(f^{(1)}_{40,6})$, $\varphi_7(f^{(1)}_{40,7})=0$, $\varphi_8(f^{(1)}_{40,8})=0$.

Remark 3. Note that in each case from (2)–(6) the last polynomial contributes only multiplicity one, because only such forms of polynomials come from Jacobi polynomials for codes.

Remark 4. One also sees that there are not many coset weight distributions in each weight from 0 to 8, if we take account of the fact that coset weight enumerators are polynomials with non-negative integer coefficients together with the above remark. For instance there are exactly 58 types of possible coset weight enumerators of weight 2.

7. Explicit results

Our strategy in determining the coset weight distributions and the covering radius of a given $[40,20,8]$ code $\mathscr{C}$ is first to search rigid vectors $\mathbf{v}\in\mathbb{F}_2^{40}$ of various weights. By [10, 2] we know that

$$6\leqslant t(\mathbf{C})\leqslant 8.$$

Thus, we have only to search rigid vectors of weights up to 8. With Proposition 9, we can easily judge whether a given vector $\mathbf{v}$ is rigid or not by examining the intersection numbers $\mathbf{v}*\mathbf{u}$ for $\mathbf{u}\in\mathbf{C}_8$ (the set of codewords of weight 8) or $\mathbf{u}\in\mathbf{C}_{12}$. This information together with the Facts 1–8 is enough to determine Jacobi polynomial $Jac(\mathbf{C},\mathbf{v}\,|\,X,Z)$. The number of different cosets with the assigned coset weight distribution is obtained by using Theorems 6 and 7. By this process we exhaust all coset weight distributions of various weights, and consequently we know the covering radius of the code $\mathbf{C}$. Note that for the determination of the covering radius of a code it is sufficient to consider only the existences of cosets of weights 7 and 8, in viewing the above inequality for $t(\mathbf{C})$ and Proposition 2.

We tried many binary $[40,20,8]$ codes. Here we give two instances of the computation. One code is chosen from [17] (the first code in it), and another is a binary $[40,20,8]$ code with trivial automorphism group (No. 103 of the Table 2 in [7]). These two codes are denoted by $\mathscr{C}_1$ and $\mathscr{C}_2$, respectively. Before giving the tables we briefly explain our process.

The first row indicates the weights of the vectors in the coset. In any binary $[40,20,8]$ code $\mathbf{C}$, there is $\binom{40}{0}=1$ Jacobi polynomial of index 0, i.e. the weight enumerator $W_{\mathbf{C}}(X)$, and there are $\binom{40}{1}=40$ rigid vectors $\mathbf{v}$ of weight 1 with the identical coset weight enumerator $\varphi_1(f_{40,1})$. For code $\mathscr{C}_1$ in [17] there are 380 rigid vectors $\mathbf{v}$ with $Jac(\mathscr{C}_1,\mathbf{v}\,|\,X,Z)=f^{(2)}_{40,2}+12f^{(1)}_{40,2}$, there are 380 rigid vectors $\mathbf{v}$ with $Jac(\mathscr{C}_1,\mathbf{v}\,|\,X,Z)=f^{(2)}_{40,2}+9f^{(1)}_{40,2}$, and there are 20 rigid vectors $\mathbf{v}$ with $Jac(\mathscr{C}_1,\mathbf{v}\,|\,X,Z)=f^{(2)}_{40,2}$. These polynomials yield the coset weight distributions of the cosets of weight 2 in Table 3.

Table 3
Distribution of weights in the cosets of the $[40, 20, 8]$ code of $\mathscr{C}_1$

i Coset weight	0	1	2	3	4	5	6	7	8	9	10	11	12	Number of different cosets
0	1								285				21280	1
1		1						57		228		6384		40
2			1				12		90		1973		9188	380
2			1				9		96		1988		9152	380
2			1				0		114		2033		9044	20
3				1		0		21		619		4125		760
3				1		1		24		600		4124		2280
3				1		2		27		581		4123		6840
4					1		0		168		1600		10620	190
4					1		3		162		1585		10656	6840
4					1		4		160		1580		10668	15960
4					1		7		154		1565		10704	29640
4					1		8		152		1560		10716	20520
4					2		0		176		1536		10680	285
4					2		3		170		1521		10716	4560
4					2		4		168		1516		10728	3420
4					3		0		184		1472		10740	570
5						1		35		525		4415		174648
5						2		38		506		4414		155040
5						3		41		487		4413		52440
6							3		154		1649		10596	46740
6							4		152		1644		10608	72390
6							7		146		1629		10644	10580
6							8		144		1624		10656	94050
6							11		138		1609		10692	47880
6							12		136		1604		10704	47310
6							15		130		1589		10740	15504
6							16		128		1584		10752	3705
6							20		120		1564		10800	171
7								32		544		4416		132240
8									160		1664		10560	2907

In $\mathbf{C}_1$ there arise 12 different rigid Jacobi polynomials of index 5. These polynomials induce three different coset weight enumerators $\varphi_5(f^{(3)}_{40,5})$, $\varphi_5(f^{(3)}_{40,5}) + \varphi_5(f^{(2)}_{40,5})$ and $\varphi_5(f^{(3)}_{40,5}) + 2\varphi_5(f^{(2)}_{40,5})$. By comparing the frequencies of the Jacobi polynomials and the coefficient of the lowest power of X in the coset weight enumerator we get the number of different cosets with the coset weight distributions $\varphi_5(f^{(3)}_{40,5})$, $\varphi_5(f^{(3)}_{40,5}) + \varphi_5(f^{(2)}_{40,5})$ and $\varphi_5(f^{(3)}_{40,5}) + 2\varphi_5(f^{(2)}_{40,5})$, respectively. This explains the rows for the cosets of weight 5. In similar ways other rows are explained.

For the code $\mathscr{C}_2$ we only give the table of coset weight distributions without giving explanations. Table 4 shows that these two codes have covering radius 8.

Recently, Harada (a graduate student in Okayama Univ.) informed us a binary $[40, 20, 8]$ code with covering radius 7, and we computed the full coset weight

Table 4
Distribution of weights in the cosets of the $[40, 20, 8]$ code of $\mathscr{C}_2$

i Coset weight	0	1	2	3	4	5	6	7	8	9	10	11	12	Number of different cosets
0	1								285				21280	1
1		1						57		228		6384		40
2			1				4		106		2013		9092	65
2			1				7		100		1998		9128	206
2			1				10		94		1983		9164	241
2			1				13		88		1968		9200	168
2			1				16		82		1953		9236	75
2			1				19		76		1938		9272	22
2			1				22		70		1923		9308	3
3				1		0		21		619		4125		1328
3				1		1		24		600		4124		3462
3				1		2		27		581		4123		3216
3				1		3		30		562		4122		1460
3				1		4		33		543		4121		384
3				1		5		36		524		4120		30
4					1		0		168		1600		10620	379
4					1		1		166		1595		10632	1816
4					1		2		164		1590		10644	4150
4					1		3		162		1585		10656	7416
4					1		4		160		1580		10668	10126
4					1		5		158		1575		10680	11127
4					1		6		156		1570		10692	10564
4					1		7		154		1565		10704	9107
4					1		8		152		1560		10716	6932
4					1		9		150		1555		10728	4924
4					1		10		148		1550		10740	3164
4					1		11		146		1545		10752	1859
4					1		12		144		1540		10764	1132
4					1		13		142		1535		10776	580
4					1		14		140		1530		10788	294
4					1		15		138		1525		10800	155
4					1		16		136		1520		10812	47
4					1		17		134		1515		10824	23
4					1		18		132		1510		10836	6
4					1		19		130		1505		10848	1
4					2		0		176		1536		10680	194
4					2		1		174		1531		10692	896
4					2		2		172		1526		10704	1956
4					2		3		170		1521		10716	2628
4					2		4		168		1516		10728	2854
4					2		5		166		1511		10740	2500
4					2		6		164		1506		10752	1868
4					2		7		162		1501		10764	1244
4					2		8		160		1496		10776	696
4					2		9		158		1491		10788	370
4					2		10		156		1486		10800	140
4					2		11		154		1481		10812	44

Table 4 (*Continued*)

i Coset weight	0	1	2	3	4	5	6	7	8	9	10	11	12	Number of different cosets
4					2		12		152		1476		10824	22
4					2		13		150		1471		10836	2
4					3		0		184		1472		10740	60
4					3		1		182		1467		10752	201
4					3		2		180		1462		10764	408
4					3		3		178		1457		10776	498
4					3		4		176		1452		10788	390
4					3		5		174		1447		10800	309
4					3		6		172		1442		10812	90
4					3		7		170		1437		10824	24
4					3		8		168		1432		10836	6
4					4		0		192		1408		10800	8
4					4		1		190		1403		10812	44
4					4		2		188		1398		10824	56
4					4		3		186		1393		10836	56
4					4		4		184		1388		10848	24
5						1		35		525		4415		32768
5						2		38		506		4414		80640
5						3		41		487		4413		35840
5						4		44		468		4412		6720
5						6		50		430		4410		4480
6							6		148		1634		10632	215040
6							8		144		1624		10656	160160
6							14		132		1594		10728	53760
6							16		128		1584		10752	5040
6							32		96		1504		7244	280
7								32		544		4416		67200
8									160		1664		10560	6720

distributions of the code. However we do not give the result. Instead we leave a problem for the readers:

Is there any binary $[40, 20, 8]$ code with covering radius 6?

The answer may be negative.

Addendum: The problem raised in the paper is answered negatively so that there is any binary $[40, 20, 8]$ code having covering radius equal to or greater then 7. This result is contained in a paper "M. Ozeki, Two results on the covering radius problem for doubly even extremal binary self-dual codes, preprint, 1999.

References

[1] E.F.Assmus, Jr., H.F. Mattson, Jr., New 5-designs, J. Combin. Theory Ser. A 6 (1969) 122–151.

[2] E.F. Assmus, Jr., V. Pless, On the covering radius of extremal self-dual codes, IEEE Trans. Inform. Theory IT-29 (1983) 359–363.

[3] E. Bannai, M. Ozeki, Construction of Jacobi forms from certain combinatorial polynomials, Proc. Japan Acad. Ser. A 72 (1996)12–15.
[4] E. Bannai, E. Bannai, M. Ozeki, S. Teranishi, Rings of simultaneous invariants for the MacWilliams–Gleason group, in preparation.
[5] G. Batut, D. Bernardi, H. Cohen, M. Olivier, PARI-GP (a computer algebra system).
[6] R.A. Brualdi, V. Pless, Weight enumerators of self-dual codes, IEEE Trans. Inform. Theory 37 (1991) 1222–1225.
[7] F.C. Bussemaker, V.D. Tonchev, Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20, Discrete Math. 82 (1990) 317–321.
[8] J.H. Conway, V. Pless, N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, J. Combin. Theory Ser. A 60 (1992) 183–195.
[9] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer, Berlin, 1988.
[10] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. and Control 23 (1973) 407–438.
[11] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Re. Rep. Suppl. 10 (1973).
[12] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in: Actes Congres Int. de Mathematique 1970, 3 Gauthier-Villars, Paris, 1971, pp. 211–215.
[13] V.I. Iorgov, Binary self-dual codes with automorphisms of odd order, Problems Inform. Transmission 19 (1983) 260–270.
[14] D.M. Ivanov, Cosets of an extremal binary code of dimension 48, J. Sov. Math. 63 (1993) 664–670.
[15] F. Klein, Vorlesungen über das Ikosaeder, Birkhäuser, B.G.Teubner, Basel, 1993.
[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[17] M. Ozeki, Hadamard matrices and doubly even error correcting codes, J. Combin. Theory Ser. A 44 (1987) 274–287.
[18] M. Ozeki, Examples of even unimodular extremal lattices of rank 40 and their Siegel theta series of degree 2, J. Numer. Theory 28 (1988) 119–131.
[19] M. Ozeki, On the relation between the invariants of a doubly even self-dual binary code C and the invariants of the even unimodular lattices L(C) defined from the code C, in: Meeting on Algebraic Combinatorics, Suuri Kaiseki Kenkyuusho Koukyuuroku No. 671, Research Institute of Mathematical Sciences in Kyouto Univ, 1988.
[20] M. Ozeki, Determination of the ring of simultaneous invariants for a group associated with MacWilliams identity (an intermediate report of a joint work with E. Bannai), in: Meeting on algebraic combinatorics, Suuri Kaiseki Kenkyuusho Koukyuuroku No. ??? Research Institute of Mathematical Sciences in Kyouto Univ, 1995, unpublished.
[21] M. Ozeki, On the notion of Jacobi polynomials for codes, Math. Proc. Cambridge Philos. Soc. 121 (1997) 15–30.
[22] V. Pless, A classification of Self-Orthogonal Codes over GF(2), Discrete Math. 3 (1972) 209–246.
[23] V. Pless, An Introduction to the Theory of Error-Correcting Codes, Wiley-Interscience, New York, 1982.
[24] V. Pless, N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory Ser. A 18 (1975) 313–335.
[25] I. Schur, Vorlesungen über Invariantentheorie, Springer, 1968, Berlin.
[26] G.C. Shephard, J.A. Todd, Finite unitary reflection groups, Canad. J. Math. 5 (1953) 364–383.
[27] N.J.A. Sloane, Error-correcting codes and invariant theory: new applications of a nineteenth-century technique, Amer. Math. Mon. 84 (1977) 82–107.
[28] N.J.A. Sloane, Self-dual codes and lattices, in Relations between Combinatorics and Other Parts of Mathematics, Proc. Symp. in Pure Math. 34 (1979) 273–308.
[29] V.D. Tonchev, Hadamard-type block designs and self-dual codes, Problems Inform. Transmission 19 (1983) 270–274.
[30] B.B. Venkov and D. M. Ivanov, Combinatorial properties of extremal doubly-even codes of length 48, J. Sov. Math. 57 (1991) 3459–3462.